INFORMATION TECHNOLOGY:
Lack of Bureau Connectivity Remains A Weakness In Treasury Communications System's Disaster Recovery Capability

OIG-03-079 April 28, 2003

Office of Inspector General

****

The Department of the Treasury

Contents

Appendices

Abbreviations

AOF	Alternate Operating Facility
ASMS	Automated Security Management System
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
DNS	Domain Name Server
DO	Departmental Offices
FMS	Financial Management Service
FY	Fiscal Year
INMS	Integrated Network Management System
IRS	Internal Revenue Service
KMC	Key Management Center
NOC	Network Operating Center
OIG	Office of Inspector General

Contents

OMB	Office of Management and Budget
PMO	Program Management Office
PVC	Private Virtual Circuit
SOP	Standard Operating Procedure
TCC	Treasury Communications System Communications Center
TCS	Treasury Communications System
TCS-MCC	TCS Back-Up Facility-Martinsburg, West Virginia
TCS-W2	TCS McLean, Virginia
TIAS	TCS Internet Access Solution
Treasury	Department of the Treasury
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network

Drew Ladner
Deputy Assistant Secretary for Information Systems
and Chief Information Officer
Department of the Treasury

The Office of Inspector General's (OIG) Annual Audit Plan for Fiscal Year (FY) 2002 included the audit, *Disaster Recovery Exercises*. This review was classified as a high priority audit in response to the events that occurred on September 11, 2001. Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. The Office of Management and Budget (OMB) requires that controls for major applications and general support systems must provide for contingency planning and/or continuity of support. A backup facility can provide the capabilities to replicate and restore critical applications and functions, in order to resume operations in the event of a disaster.

The lack of an emergency backup facility for the Treasury Communications System (TCS) in McLean, Virginia (TCS-W2) was identified as a security weakness in a prior OIG audit report.[1] As a result, we recommended that the Department create a secondary TCS Communications Center (TCC), with adequate physical security. The weakness cited in the report was subsequently classified as a material weakness in the Department of the Treasury's (Treasury) FY 2000 Accountability Report.

In response to the lack of a backup facility being declared a material weakness, Treasury developed a remediation plan to assist in establishing a disaster recovery site to support TCS' Continuity

[1] *Audit of Treasury Communications System Automated Information System Security Program*, dated February 1999, (OIG-99-039).

of Operations Plan (COOP). The remediation plan was implemented in three phases beginning in January 2002. An acceptance test was conducted at the end of the first two phases to evaluate whether disaster recovery capabilities and critical system functionalities were working as designed.

The objectives of this review were to determine if the Department implemented our prior audit recommendation and evaluate TCS' disaster recovery acceptance testing. In May and October 2002, we observed the acceptance testing for phases one and two conducted at TCS' primary operating facility in McLean, Virginia, and the backup facility in Martinsburg, West Virginia (TCS-MCC). During these observations, we evaluated TCS' ability to start up critical backup systems; and resume processing at TCS-MCC after the Private Virtual Circuit[2] (PVC) between TCS-W2 and TCS-MCC was disabled. Specifically, we determined whether TCS was able to (1) replicate data from primary systems at TCS-W2 to stand-by backup systems at TCS-MCC; (2) promote stand-by backup systems to primary systems; (3) run critical applications; and (4) perform key operations and functions (e.g., opening trouble tickets, generating reports, retrieving files and e-mails, dialing into remote routers, and establishing connection with Voice Over Internet Protocol (VoIP) phones). Because bureaus had not established connectivity to TCS-MCC, critical functionalities, such as network monitoring, were not performed. A more detailed description of our objectives, scope, and methodology is provided in Appendix 1.

Results In Brief

TCS management has taken actions to remedy the material weakness by establishing a backup facility at TCS-MCC. In addition, TCS management succeeded in recovering critical systems during acceptance testing. Test procedures used to verify communication, key functions, and operations were also successfully executed and completed during the disaster recovery acceptance testing conducted in May and October 2002. During

[2] A PVC is a logical connection between two sites.

the tests, data from selected critical systems was backed up at TCS-W2, and replicated to systems at TCS-MCC. After disabling the network communication between TCS-W2 and TCS-MCC, the recovery team at TCS-MCC began executing the recovery procedures by (1) promoting the backup Domain Name Server (DNS) to primary; (2) configuring the system to point to the DNS for internet protocol address resolution; and (3) opening individual applications and querying records previously created from systems at TCS-W2.

Although disaster recovery capabilities exist for TCS, we identified a number of weaknesses that need attention:

- Bureaus had not established connectivity to TCS-MCC to ensure networking services would not be interrupted in the event of a disaster.
- Performance testing was not conducted for systems at TCS-MCC.
- Disaster recovery exercises were not conducted, and disaster recovery standard operating procedures (SOP) were not documented.
- Access to the Network Operating Center (NOC) at TCS-MCC was not restricted.

The purpose of a backup facility is to minimize service interruption in the event of a disaster. Although a backup capability exists, without connectivity, TCS-MCC cannot provide essential services (e.g., network and router management, Internet access, Virtual Private Network (VPN), X.500 Directory, and e-mail) to the bureaus. The Chief Information Officer's (CIO) memorandum dated October 2002, required bureaus to establish connectivity between TCS-MCC and both their headquarters and alternate operating facilities (AOF). Each bureau was required to submit its plan and service order to TCS for establishing connectivity by October 31, 2002. As of November 2002, no circuits were installed and only four bureaus (Departmental Offices (DO), the Financial Management Service (FMS), Office of Thrift Supervision, and the U.S. Customs Service) indicated that they would fully

comply with the requirement to establish connectivity with TCS-MCC.

Our report includes the following recommendations that, in our opinion, will assist the Treasury in remedying the deficiencies identified above. Specifically, we are recommending the CIO:

- Ensure bureau connectivity to TCS-MCC is established for uninterrupted services.
- Conduct performance evaluations on systems at TCS-MCC to ensure that the systems are operating as designed and have the capacity to handle normal processing activity in the event of a disaster.
- Conduct disaster recovery exercises to prepare staff for disasters and to evaluate the effectiveness of TCS' disaster recovery plan; and document disaster recovery standard operating procedures.
- Improve security for the TCS-MCC NOC.

The intent of our prior audit report[3] recommendation was to ensure that, with the creation of a backup facility, TCS could continue to provide uninterrupted services in the event of a disaster. Although TCS established TCS-MCC as a backup facility, TCS-MCC requires connectivity with the bureaus to provide essential services or minimize service interruptions. The Treasury may consider downgrading the material weakness associated with the lack of TCS' backup facility when (1) all bureaus have established connectivity to TCS-MCC, and (2) disaster recovery exercises are successfully conducted.

In its response to our draft report, TCS management concurred with all our findings and recommendations. In addition, TCS management has already commenced efforts to implement our recommendations. Their response is summarized and evaluated in the body of this report and included, in detail, in Appendix 4, Management Comments.

[3] See the report cited in footnote 1.

Background

The TCS provides the framework for Treasury's information infrastructure. This infrastructure enables a wide selection of applications, which include simplified tax and wage reporting, linking law enforcement agencies and public safety, and the development of an international trade database. The TCS provides services to more than 4,500 locations around the nation with approximately 120,000 users operating on a single integrated network. The mission of TCS is to design, build, manage, and operate Treasury's Wide Area Communications Network. There are five components of TCS:

- Network and Services – The Network and Services component consists of an Asynchronous Transfer Mode super backbone that provides integrated data, voice, and video capabilities.
- TCC – The TCC component houses the integrated network management system, the automated security management system, the operations and maintenance staff, and the executive agent and bureau representatives.
- Integrated Network Management System (INMS) – The INMS system component consists of an open system compliant application that provides network performance monitoring and management, help desk operations, trouble ticket management, automated service ordering, configuration management, network change management, and billing.
- Automated Security Management System (ASMS) – The ASMS provides for a secure network with system link level encryption and C2 security level controlled access protection.
- Internet Services – The Internet Services component includes services such as the electronic commerce application; web application server hosting; e-mail; X.500 Directory service; DNS; firewall management for public internet access; VPN; network management and control; and the Internet service provider digital subscriber line.

The lack of a TCC emergency backup facility was identified as a security weakness in a prior OIG audit report. In the report, the

OIG recommended that Treasury create a secondary TCC site with adequate physical security. In September 2001, Treasury set about to establish a disaster recovery site to support TCS' COOP. A remediation plan was developed and then implemented in three phases. In January 2002, Treasury began assembling the TCS-MCC. The three phases of the remediation plan are as follows:

- Phase-one consisted of two parts. Part-one, phase-one established interim capability and was completed in January 2002. The completion of this part of phase-one provided the capability to operate TCS functions remotely at TCS-MCC. Part-two, phase-one established partial capability and was completed in April 2002. The completion of part-two provided the necessary infrastructure to support the TCS Internet Access Solution (TIAS) initial operational capability, Key Management Center (KMC), and emergency ticket and e-mail functionality.

- Phase-two, which provided limited capability, was completed in October 2002. With the completion of this phase, the infrastructure established at TCS-MCC allowed the site to duplicate the functions of TCS-W2. Phase-two also provided for functional database synchronization, and the capability to operate autonomously in the event of a disaster.

- Phase-three is currently in process. Once completed, TCS will have full operational capability to implement its COOP. The bureaus are required to establish connectivity to the TCS-MCC infrastructure during this phase. There are plans to increase TCS-MCC's capacity to support future requirements in this phase.

In addition, acceptance testing was conducted at the completion of the first two phases to ensure that disaster recovery capabilities would work as designed. Phase-one and phase-two of the TCS disaster recovery capability implementation are illustrated in Appendix 2.

Results and Recommendations

Results — Weaknesses Could Impair TCS' Disaster Recovery Capabilities

TCS management has taken actions to remedy the material weakness by establishing a backup facility at TCS-MCC. In addition, TCS was successful in recovering critical systems during acceptance testing. During our review, we identified a number of controls that had been implemented which strengthen TCS' disaster recovery capability and minimize unexpected service disruption in the event of disaster. For example:

- The TCS-MCC operates in a hot failed-over mode[4] with duplicate systems serving as backups for primary systems at TCS-W2. In the event of a disaster, operating in a hot failed-over mode enables a quick turn around to restore critical systems and services. Data is also automatically replicated from the TCS-W2 site to the TCS-MCC site.

- The CIO memorandum issued in October 2002, mandates that all bureaus establish connectivity to TCS-MCC from both its headquarters and AOF. Frame relay circuits should be installed between the bureaus and TCS-MCC. When the circuits are installed, traffic can be redirected with a network software change in the event of disaster.

- A draft TCS disaster recovery plan was developed to restore critical services and functions within the 12-hour timeframe of a declared disaster. The draft disaster recovery plan includes the requirements for maintaining TCS-MCC; the organization, resources, and staffing required to effectively respond to a disaster; and the process to restore systems and begin AOF operations.

[4] A mode of operation for failure tolerant systems in which the component has failed and its functions have been assumed by a redundant component.

Although TCS management established a backup facility at TCS-MCC, we identified weaknesses in TCS' disaster recovery capabilities that would impact TCS and Treasury bureaus in the event of disaster or unplanned disruption at TCS-W2.

Bureaus Had Not Established Connectivity To TCS-MCC

All bureaus currently receive TCS services through connections to TCS-W2 from their individual headquarters. Although TCS-MCC is established as the backup facility for TCS-W2, without direct bureau connectivity to TCS-MCC, TCS cannot provide its full services to the bureaus in the event of a disaster. For instance, in the event of a disaster and without bureau connectivity to TCS-MCC, (1) TCS cannot proactively monitor bureaus' routers or manage the telecommunication services and circuits from TCS-MCC; (2) all bureaus will loose Internet access, X.500 Directory, and e-mail services; and (3) several bureaus (Bureau of Engraving and Printing, Financial Crimes Enforcement Network, FMS, the Internal Revenue Service (IRS), and Office of the Comptroller of the Currency) will experience service interruption on application and web hosting/housing. Appendix 3 lists the service interruption to the bureaus in the event of a disaster where connectivity to TCS-MCC is not established. Bureaus need to establish connectivity to TCS-MCC to ensure networking services are not interrupted.

Performance Testing Was Not Conducted

Network traffic and transactions are equally distributed and processed among the TCS-W2 and TCS-MCC sites. The TCS-MCC was established as a backup facility to minimize service interruptions and provide essential services in the event of a disaster. Thus, both network connectivity to TCS-MCC and the systems at TCS-MCC must be capable of individually processing all TCS network traffic and transactions in the event of a disaster. Since connectivity was not established between TCS-MCC, bureaus' headquarters, and AOFs, performance evaluations were not conducted on systems at TCS-MCC. Without a performance evaluation, there is no guarantee that the systems at TCS-MCC

have the capacity to handle normal processing activity in the event of a disaster.

Disaster Recovery Plan Was Not Tested And Site Transitioning SOPs Were Not Documented

Although TCS management was successful in recovering all critical systems selected for acceptance testing, we found that TCS management had not conducted disaster recovery exercises nor documented disaster recovery SOPs for transitioning TCS-MCC from a secondary site to a primary site. We found that TCS' disaster recovery plan was drafted, but was not finalized, approved, or tested. The disaster recovery plan should be tested periodically to ensure the plan would work as intended. The lack of disaster recovery exercise and training increases the risk of an unsuccessful recovery, or delaying the time of recovery. The SOPs are needed to systematically guide the operators in promoting a backup facility to a primary facility.

Access Was Not Restricted And Logged At TCS-MCC

The TCS-MCC is located in the IRS data room and shares the space with DO and Emergency Preparedness staff. Currently, there are no perimeter walls separating the TCS area from the rest of the IRS data room. In addition, physical access to the TCS area is not logged. Therefore, anyone with physical access to the IRS data room has unrestricted access to the TCS area. Although there are strong physical controls at TCS-MCC NOC, access to the TCS area should be restricted to need-to-know, or only those personnel who require access to perform their duties.

OMB Circular A-130, *"Management of Federal Information Resources"*, establishes policy for the management of federal information resources. Appendix III, *"Security of Federal Automated Information Resources"*, of this circular establishes a minimum set of controls to be included in federal automated information security programs. According to Appendix III, managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to

function or a general support system failure. Experience has demonstrated that testing a recovery plan significantly improves its viability. Untested plans, or plans not tested for a long period of time, may create a false sense of ability to recover in a timely manner. Also, per the Federal Information System Controls Audit Manual, physical access should be limited to personnel with a legitimate need to perform their duties.

Since TCS is the conduit for disseminating Treasury information and data, any major TCS service disruption can impede Treasury and bureaus' operations and missions. In the event of a disaster, inadequate recovery capabilities would cause mission critical operations to cease. Conducting disaster recovery exercises ensures that the disaster recovery plan can be successfully applied and evaluated for effectiveness, revealing any shortcomings and providing valuable training experience to team members. Restricted access to the Treasury area at TCS-MCC is critical to controlling the overall integrity of information systems and data and also reducing the risk of damage to the systems from malicious acts.

Recommendations

The Treasury CIO should:

1. Ensure bureau connectivity to TCS-MCC is established for uninterrupted services.

Management response:

TCS management concurred with this recommendation. The TCS Program Management Office (PMO) will continue to track bureau progress in establishing connectivity to TCS-MCC. Bureau connectivity status is shared with Treasury components at quarterly Information Sharing Sessions. The TCS PMO will also provide status reports regarding the progress bureaus make on their connectivity to TCS-MCC during monthly CIO Council meetings. In addition, operations personnel at the TCS PMO are continuing to work with bureaus that are not in compliance

regarding connectivity to TCS-MCC by assisting them in ordering service to TCS-MCC. The target date for bureau connectivity is November 2003.

2. Conduct performance evaluations on systems at TCS-MCC to ensure that the systems operate as designed and have the capacity to handle normal processing activity in the event of a disaster.

Management Response:

TCS management concurred with this recommendation. Performance load testing is scheduled for FY03 after bureau connectivity is established to TCS-MCC. Critical TCS applications will continue to be evaluated to ensure that TCS-MCC can handle the traffic load through site simulation and testing. Furthermore, TCS-MCC's operating procedures and traffic capacity are continually evaluated based on Treasury contingencies. The target date for this action is December 2003.

3. Conduct disaster recovery exercises to prepare staff for disasters and to evaluate the effectiveness of TCS' disaster recovery plan; and document disaster recovery standard operating procedures.

Management Response:

TCS management concurred with this recommendation. Continuity of operations exercises are being conducted, and will continue to be planned and conducted based on the availability of resources and travel funds. The TCS Disaster Recovery Plan has been updated as of April 2003 and is currently under review. A TCS-level disaster recovery exercise is planned in calendar year 2003 upon completion of bureau connectivity into TCS-MCC. The TCS PMO will continue to validate and verify emergency business processes and operating procedures in TCS' COOP, disaster recovery plan, and operating guides during all exercises. The target date for this action is November 2003.

4. Improve security for the TCS-MCC NOC.

Management Response:

TCS management concurred with this recommendation. To control and monitor access to the TSC-MCC area, a steel mesh cage and a closed-circuit television system will be installed. The closed-circuit television system will be monitored by Internal Revenue Service Security Personnel in the TCS-MCC Annex. In addition, a stand-alone electronic access control system will be installed to meet Treasury security requirements. The target date for this action is June 2003.

OIG Comment:

The OIG agrees that the formal steps TCS management has taken, and plans to take, satisfies the intent of the recommendations.

The intent of our prior audit report recommendation was to ensure that, with the creation of a backup facility, TCS could continue to provide uninterrupted services in the event of a disaster. Although TCS management established TCS-MCC as a backup facility, TCS-MCC requires connectivity with Treasury bureaus to provide essential services or minimize service interruptions. The Treasury may consider downgrading the material weakness associated with the lack of a TCS backup facility when all bureaus have established connectivity to TCS-MCC, and disaster recovery exercises are successfully conducted.

* * * * * *

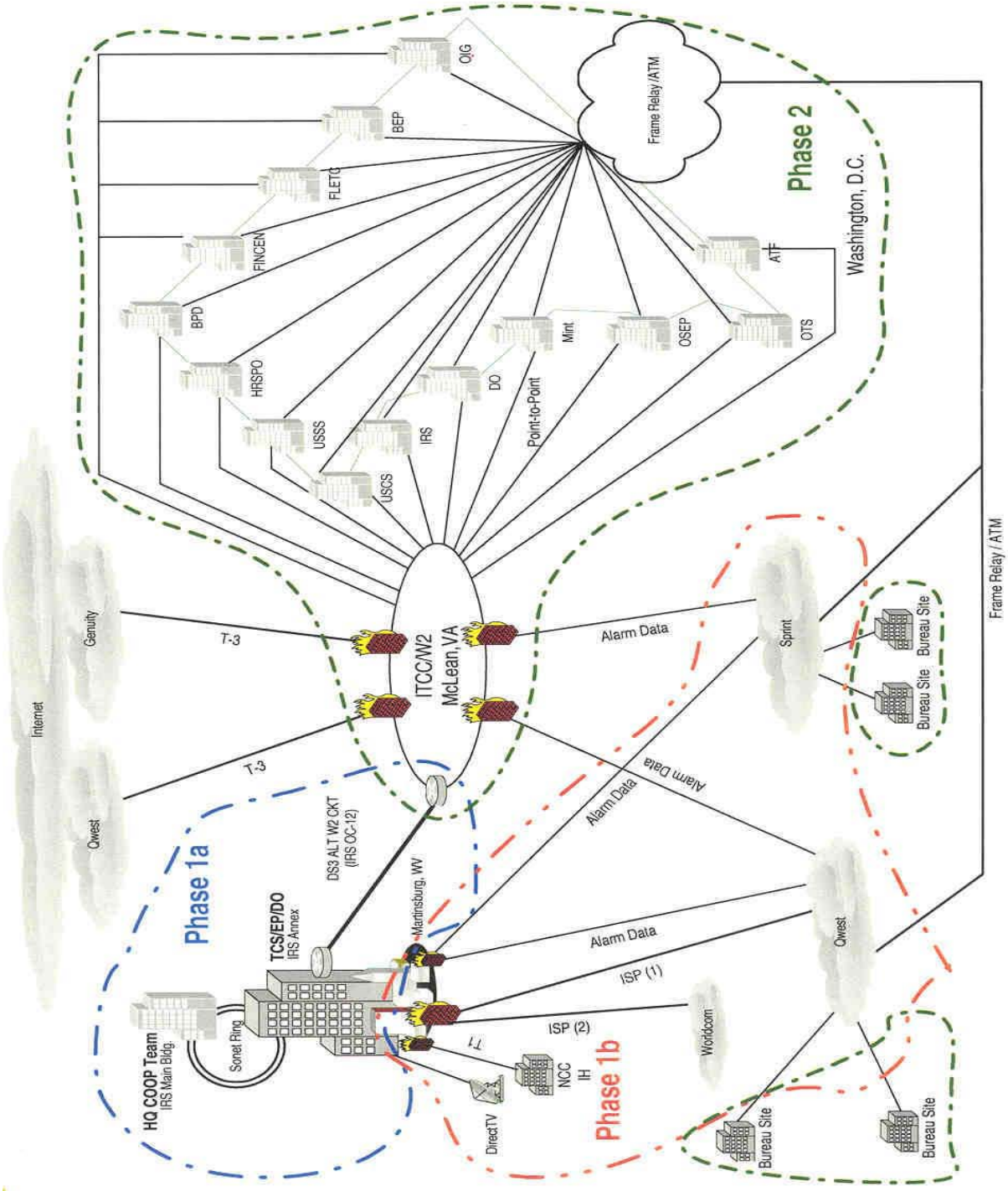
I would like to extend my appreciation to TCS for the cooperation and courtesies extended to my staff during the review. If you have any questions, please contact me at (202) 927-5774, or Joseph A. Maranto, Audit Manager, Office of Information Technology Audits, at (202) 927-5014. Major contributors to this report are listed in Appendix 5.

/s/
Louis C. King
Director, Office of Information Technology Audits

The objectives of this review were to determine if the Department implemented our prior audit recommendation, and evaluate the Department's disaster recovery capabilities at TCS-MCC. These objectives were accomplished by identifying if TCS had taken corrective actions to remedy the weakness identified, and evaluating TCS' disaster recovery capabilities by observing the acceptance testing conducted at TCS-MCC.

We observed TCS' disaster recovery acceptance testing for phases one and two in Martinsburg, West Virginia (i.e., TCS-MCC) in May and October 2002, and in McLean, Virginia (i.e., TCS-W2) in October 2002. Data used to recover critical systems at TCS-MCC was created at TCS-W2 and replicated at TCS-MCC. Testing resumed at TCS-MCC after the PVC between TCS-W2 and TCS-MCC was disabled. Once the PVC was disabled, we observed operators at TCS-MCC began the recovery process by promoting the local DNS server from backup status to primary and entered router changes. After promoting major systems from backup to primary, we observed operators using test procedures to restore data and perform key operations, such as retrieving and viewing records previously created at TCS-W2, testing key functions, operations, and communication. Testing was performed for NT servers, Network Information Service Plus, NFS, Oracle, VoIP, INMS applications, X.500, VPN, and Security Management applications.

The results of this report are based solely on our observation of the acceptance testing at TCS-MCC. We only evaluated TCS' ability to restore critical systems selected. We did not evaluate TCS-MCC's disaster recovery capabilities, as the backup facility is isolated without bureau connectivity.


Phase 2
Washington, D.C.
Frame Relay /ATM
OIG
BEP
FLETC
FINCEN
BPD
HRSPO
USSS
USCS
IRS
DO
Point-to-Point
Mint
OSEP
OTS
ATF
ITCC/W2
McLean, VA
T-3
Genuity
Internet
Qwest
Alarm Data
Sprint
Bureau Site
Bureau Site
Frame Relay / ATM
Phase 1a
TCS/EP/DO
IRS Annex
DS3 ALT W2 CKT
(IRS OC-12)
Martinsburg, WV
HQ COOP Team
IRS Main Bldg
Sonet Ring
ISP (1)
ISP (2)
T-1
DirecTV
NCC
IH
Phase 1b
Worldcom
Qwest
Bureau Site
Bureau Site

Appendix 3
Services Impacted Without Bureau Connectivity To TCS-MCC

Services/Bureaus	TTB	BEP	BPD	DO	FinCEN	FMS	IRS	Mint	OCC	OIG	OTS
International/ OCONUS	●						●				
Customer Servie & Support	●	●	●	●	●	●	●	●	●	●	●
Network Management	●	●	●	●	●	●	●	●	●	●	●
E-Commerce Authentication						●	●				
WAN Infrastructure Upgrades / Modernization	●	●	●	●		●	●	●	●		●
Communications Engineering / Capacity Planning	●	●	●	●	●	●	●	●	●	●	●
Secure WAN Services	●	●	●	●	●	●	●	●	●	●	●
Virtual Private Network (VPN) TRW / Verizon							●				
Managed Firewall Services	●			●	●	●	●		●	●	
Directory Services (White Pages Initiative)	●	●	●	●	●	●		●	●	●	●
E-mail Services	●	●	●	●	●	●	●	●	●	●	●
Internet Access	●	●	●	●	●	●		●	●	●	●
Web Hosting/Housing		●			●	●	●		●		
Application Hosting					●	●	●				

Green = Functional **Yellow** = Depends on bureau's COOP capabilities
Red = Loss of Service

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220
APR 22 2003

MEMORANDUM FOR EDWARD G. COLEMAN
DIRECTOR, INFORMATION TECHNOLOGY AUDITS
OFFICE OF THE INSPECTOR GENERAL

FROM: Drew Ladner
Chief Information Officer

SUBJECT: Management Response to Draft Audit Report – "Lack of Bureau Connectivity Remains a Weakness in Treasury Communications System's Disaster Recovery Capability"

Attached is the Treasury, Chief Information Officer (CIO) response to the findings and recommendations contained in the Draft Audit Report, dated March 20, 2003.

The Treasury Communications System (TCS) Program Management Office (PMO) is committed to providing the highest level of information technology support possible to all Treasury worldwide customers (i.e., Continental US, Outside Continental US and selected international sites). The TCS Program Management Office is committed to operating and maintaining a telecommunications service in a manner that is consistent with Treasury and other Federal policies and practices. This office concurs with the recommendations in the Inspector General Draft report and management responses are hereby provided. This office looks forward to using your recommendations as a tool to enhance the services provided to the various TCS users.

We are aware of and endorse the processes for managing TCS backup facilities, security, and configuration as described in the IG report. In many cases, the TCS PMO had previously identified these issues and initiated tasks to document and remediate these issues. The findings identified in your audit report are considered extremely important to our program. Operational exigencies and a dynamic environment have consumed many of the energies and resources available to the TCS disaster recovery function. With adequate funding, these findings can be corrected. To ensure viability and continuation of the TCS disaster recovery capability, ongoing operations and maintenance funding have been included as components of the Fiscal Year 2003-2005, TCS Bureau financial planning and budget forecasting process.

Again, this office wishes to express its appreciation for your timely and thorough assessment, along with insightful and valued recommendations concerning the Treasury Communications System disaster recovery planning and implementation process.

Attachment

Management Response to Draft Audit Report "Lack of Bureau Connectivity Remains A Weakness In Treasury Communications System's Disaster Recovery Capability" (March 20. 2003)

Recommendation 1: Ensure bureau connectivity to the TCS Martinsburg Computing Center (MCC) is established for uninterrupted services.

Comments: In October 2002, the Treasury CIO directed each Bureau CIO to provide connectivity from their Headquarters and alternate operating facility sites to the TCS Alternate Operating Facility (AOF) located at Martinsburg, WV, by the end of December 2002. The TCS PMO is tracking Bureau connectivity into the TCS AOF/MCC from both their existing Bureau headquarters and their alternate operating locations. The status of this connectivity is shared with the Treasury community at quarterly Information Sharing Sessions (ISS), lead by the TCS PMO, with attendance by respective Bureau IT management representatives. The CIO Council is also periodically briefed. Bureau connectivity is currently 62 percent complete with four (4) bureaus scheduled for completion by the end of April 2003. Four (4) bureaus are pending approval and funding of their requirements by senior bureau leadership. Bureau customers are continually being made aware of the impact of their lack of action to comply with the mandate from the Treasury CIO.

Furthermore, due to the establishment of the Department of Homeland Security (DHS), the bureaus transitioning from the Treasury to the DHS have canceled their service requests for connectivity. These bureaus are the US Secret Service, US Customs Service and the Federal Law Enforcement Training Center.

Corrective Actions:

1. The TCS PMO continues to track the status of service requests and connectivity into the TCS AOF/MCC. A "stoplight" report is forwarded to CIO management for discussion during Treasury-level CIO meetings every month. A copy of the latest status is attached.

2. The TCS PMO is continuing to work with those bureaus not in compliance and to assist them in ordering the service to TCS AOF/MCC site. The TCS PMO operations support personnel have drafted several service requests for those bureaus that have not established their own service order for connectivity. The TCS PMO cannot activate these service requests until Bureau fiscal issues are resolved.

Target date of completion: November 2003.

Recommendation 2: Conduct performance evaluations on systems at TCS MCC to ensure that the systems operate as designed, and have the capacity to handle normal processing activity in the event of a disaster.

Comment: Performance load testing of critical TCS applications is scheduled as a part of the post activities to be completed during FY 03 based upon completion of Bureau connectivity into the facility. Bureau connectivity to the TCS backup facility center is still underway with a 62 percent completion rate with four (4) Bureaus scheduled for installation by the end of this month. Four (4) bureaus are pending approval and funding of this requirement.

In the event that an emergency operation is required through the TCS alternate operating facility, TCS will be able to handle the traffic load based on the reduced size of the emergency staffs operating from the Treasury Headquarters and the Bureaus' emergency relocation sites. Treasury Headquarters and the Bureaus are currently forming these emergency staffs.

Corrective Actions:

1. Conduct performance load testing of critical TCS applications during FY 03 after completion of Bureau connectivity into the AOF/MCC.

2. Continue to evaluate critical TCS applications to ensure that TCS AOF/MCC can handle the traffic load through site simulation and testing. The TCS AOF/MCC is continually staffed as a "hot" site based on current world events and situations and its operating procedures and traffic capacity are continually being evaluated based on Treasury contingencies.

Target date of completion: December 2003

Recommendation 3: Conduct disaster recovery exercises to prepare staff for disasters and evaluate the effectiveness of the TCS disaster recovery plan.

Comment: The TCS supports four different Disaster Recovery/Continuity of Operations exercises. These include:

1. **The TCS Continuity of Operations Orientation**: This exercises the emergency personnel alert and notification recall list, provides an orientation on the TCS AOF/MCC, and familiarizes all TCS personnel, both in the TCS PMO and the prime contractors, of their roles and responsibilities. The TCS PMO has conducted two successful orientation exercises and semi-annual exercises are being scheduled based on the availability of resources and travel funds.

2. **The TCS Disaster Recovery (DR)**: This is a full cut-over exercise on the TCS system. This exercise will be planned after all Bureaus have been connected into the TCS AOF/MCC. The TCS PMO plans for an exercise by the end of CY 2003 where all standard operating guides will be validated and tested.

3. **The Emergency Preparedness/Treasury HQ COOP (with TCS support)**: As required, TCS will support any Treasury-level COOP exercise at the AOF/MCC in accordance with their schedule.

4. **Departmental Offices (DO) (with TCS support)**: As required, TCS will support DO COOP or DR exercises in accordance with their schedule.

In addition, the prime contractor has provided a revised edition of the TCS Disaster Recovery plan based on changes occurring at the Treasury COOP/DR level. This edition has been expanded in the areas of standardizing processes and operating procedures under an emergency. The prime contractor is currently completing TCS AOF/MCC on-site operating guides. The TCS PMO is continually updating its version of the TCS COOP/DR plan in accordance with the changes that are evolving from Treasury Headquarters.

Corrective Actions:

1. Recurring TCS PMO COOP exercises are being conducted and will continue to be planned and conducted on a timely basis in the future based on the availability of resources and travel funds.

2. The TCS PMO completed a review of the prime contractor written Disaster Recovery Plan for FY02 and provided substantive comments based on recent changes associated with the Treasury Department COOP/DR. The TCS PMO just received the latest edition of the TCS DR Plan product for FY03 on April 4, 2003. This plan is currently under review.

3. A TCS-level Disaster Recovery Exercise is planned in CY03 upon completion of Bureau connectivity into the TCS AOF/MCC.

4. The TCS PMO will continue to validate and verify the emergency business processes and operating procedures in the TCS COOP, DR plan and operating guides during all exercises.

Target date of completion: November 2003

Recommendation 4: Improve security for the TCS MCC NOC.

Comment: The TCS AOF/MCC Network Operation Center (NOC) resides in a Level-5 secured IRS complex and building. This security consists of security-in-depth with a 24x7 security staff located at the complex's entrance to each building access. This multi-layer access controls consist of badge checks, vehicle inspections and searches, and video surveillance at the complex entrances and building accesses. However, the TCS PMO has recognized the requirement for a physical barrier to separate the TCS AOF/MCC from the IRS space within the building complex due to variation in the personnel security clearances between the Treasury and the IRS personnel. As a result, a steel meshed cage with a separate stand-alone personnel security access system is required to segment the facility as

an additional level of security. The IRS building management issues and funding transfer issues were initial barriers to the development and installation of this system.

Corrective Actions:

1. Install and establish a slab-to-slab steel mesh cage around the TCS AOF/MCC infrastructure area within the Martinsburg Computing Center (MCC) Annex in order to meet existing Treasury security requirements. In addition, install and operate a closed-circuit television system that will be monitored by IRS uniformed Security Personnel in the MCC Annex for controlled access to the TCS AOF/MCC and the Treasury Headquarters back-up infrastructure. This is being contracted through the IRS, the MCC and the GSA.

2. Install and establish a controlled, stand-alone electronic access control system for meeting Treasury security requirements.

Target date of completion: June 2003

Office of Information Technology Audits

Edward G. Coleman, Former Director
Joseph A. Maranto, IT Audit Manager
Tram J. Do, Computer Specialist
Tom Tsang, IT Auditor
Stacey Ansell, Referencer

The Department of the Treasury

Office of the Deputy Assistant Secretary for Information Systems/Chief Information Officer
Office of Accounting and Internal Control

Office of Management and Budget

Office of Inspector General Budget Examiner